製品概要

Zero Trustネットワークアクセス

Cloudflare Zero Trust、特に、Accessはチームの生産性を高め、自社ホスト、SaaS、またはWeb以外のアプリにVPNなしでアクセスするすべてのユーザーのリスクを減らします。

ハイブリッドの勤務環境に簡単かつ安全なアクセスを

インターネットネイティブなZero Trustネットワークアクセス (ZTNA)

現代の分散した勤務環境では、安全面でも分散型のアプローチが必要です。もはや会社の内外を隔てる「壁」はなく、VPNのような従来のリモートアクセスソリューションでは、現代の人々が抱くセキュリティやパフォーマンスの期待を満たすことはできません。

ZTNAは、リソースベースでリソースのIDやデバイスポスチャーなど、細かな背景情報を継続的に検証することで、デバイスや場所を問わずにあらゆるユーザーとアプリを簡単かつ安全に接続します。完全に新しいアプローチを使用することで、セキュリティとユーザーエクスペリエンスの間で「妥協する」必要はなくなりました。ZTNAなら、セキュリティとユーザーエクスペリエンスの両方を高めてビジネスに活かせます。

クラウド移行やM&Aなどの取り組み、または迅速な革新やスケーリングに関係なく、企業が変化により俊敏かつ効果的に対応することにもつながります。CloudflareはZero Trust戦略、またはセキュリティモダナイゼーション戦略の中心にあり、プログラム可能でグローバルなコネクティビティクラウドにZTNAを提供します。

80% VPN使用時のリモートアクセス対応にかかった時間の減少率 [1]

72% 以前のベンダーとの比較で、毎月のポリシー設定で削減された時間 [1]

68% 企業が従業員や請負業者の認証エクスペリエンスを効率化するために大きな影響があったと回答した割合 [1]

最新化されたアクセスでビジネスに力を与える

ユーザーエクスペリエンスを強化

最新化されたセキュリティによって、オンプレミスアプリがSaaSアプリと同じ感覚で使用できるようになり、チームの生産性が向上します。遅くて不便なVPNは不要となり、従業員からの苦情もありません。

ラテラルムーブメントを排除

アクセス許可をネットワークレベルではなく、リソース単位でコンテキストベースの最小限の特権とすることで、サイバーリスクを軽減し、攻撃対象領域を縮小します。

Zero Trustのスケーリングが容易

重要なアプリや最もリスクの高いユーザーグループを保護し、その後インターネットネイティブのZTNAを拡張してビジネス全体を保護することで、テクノロジーの効率を向上させます。

Accessの主な使用例

セキュアなハイブリッドワーク

- ★ **VPNの増強と置き換え** — Accessは従来のVPNに比べよりスピーディで安全です。セキュリティとエンドユーザーエクスペリエンスを向上するために重大なアプリの移行を開始しましょう。
- ★ **請負業者のアクセス** — クライアントレスのオプションやソーシャルIdPなどを用いて、請負業者などのサードパーティユーザーを認証します。
- **開発者のアクセス** — 権限のあるテクニカルユーザーが、パフォーマンスに影響を与えることなく、重要なインフラストラクチャに、安全にアクセスできます。

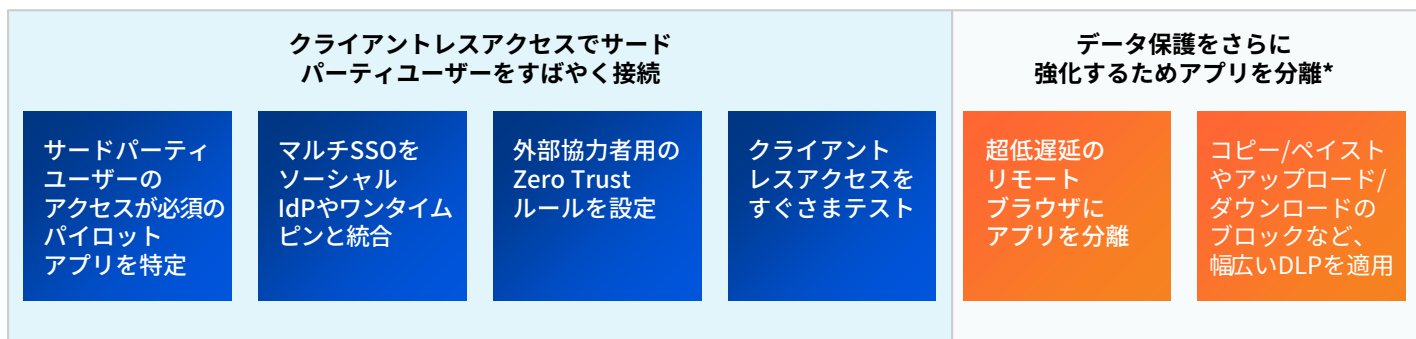
デジタルモダナイゼーションの実行

- **M&Aの取り組みを迅速化**—従来のネットワークをすべて統合することは現実的ではありません。複数のIdPを統合し、M&A中にはアプリごとに内部アクセスするアプローチを取ります。
- **クラウド移行**—クラウドへのアプリやIDのディレクトリを移行する際など、トランスフォーメーション中のビジネス持続性を保証します。
- **フィッシングに耐性があるMFA**—強力な認証（FIDO2準拠のセキュリティキーなど）をあらゆる場所に展開します。

VPNの増強および置き換えを始める

重要なアプリや高リスクユーザーを優先してZTNAをパイロット導入し、VPNを補強します。テストを促進するために、Webアプリケーションやインブラウザ のSSHにクライアントレスアクセスを使用します。徐々に高度な機能を導入し、VPNを完全に脱却する方向へ向かって、ネットワークの変化に合わせて動的な可視化を実現します。

請負業者（サードパーティ）アクセスを始める

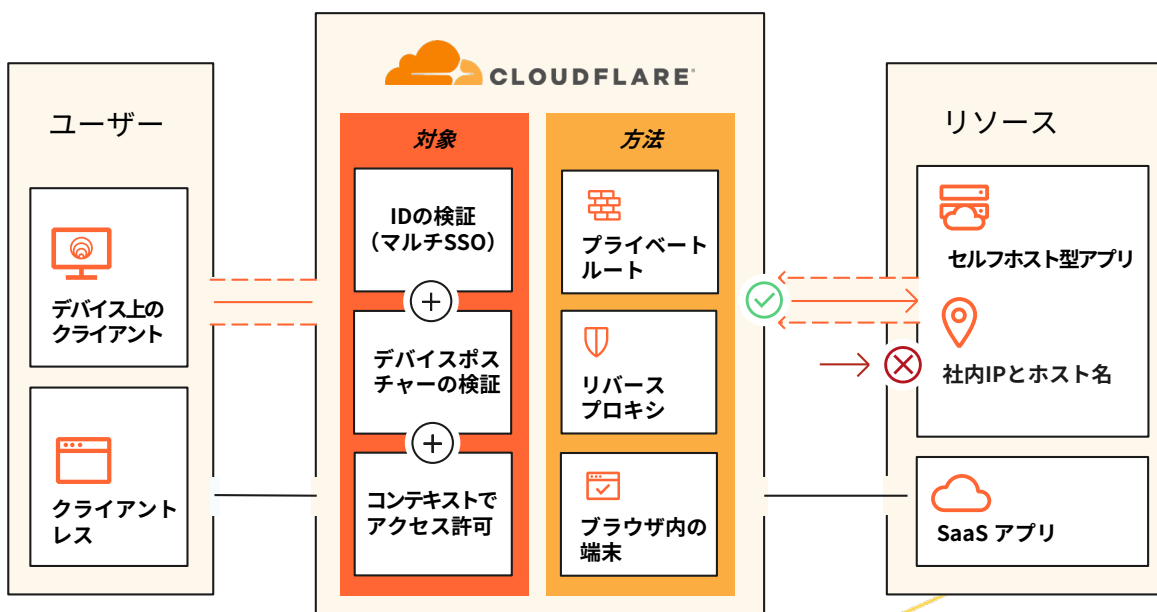
円滑なユーザーエクスペリエンスを提供しつつ、管理対象外のデバイスに起因するリスクを軽減。請負業者にエンドユーザーソフトウェアを必要としないシンプルな認証オプションを設定。さらなるデータ保護を適用するために時間をかけて高度な機能を導入。

**Zero Trustプラットフォームの他の部分で機能を使用*

Accessの仕組み

Cloudflare Accessはアイデンティティやデバイスポスチャーなど細かな背景情報を継続的に検証する柔軟な集約レイヤーで、ソフトウェア定義による境界を作り出すことで、組織のリソース全体に簡単かつ安全なアクセスを個別に提供します。ユーザーが認証を受け、すべてのアクセスポリシーの条件を満たすと、Accessは指定したセッション期間中に有効な署名付きのJSON Webトークンを発行します。Cloudflareでは構成可能なプラットフォームを介してすべてのユーザーリクエストにシングルパス検査を実施し、一元化されたポリシー管理エクスペリエンスがポリシーの変更を数秒でグローバルに拡散します。これを可能にするのが、Cloudflareのユニークなエニーキャストネットワークアーキテクチャです。

統合されたクライアントレス操作とクライアントベースの操作が、すべてのデバイスタイプを処理します。顧客データのプライバシーを保持するために、ネットワークへのトラフィックを暗号化するZero Trustサービス全体に1つのデバイスクライアントを使用します。また、クライアントレスセットアップを通じて企業外のデバイスにも簡単かつ安全にアクセスできるようにします。ZTNA、DNS、市場最先端のWAF、DDoS保護サービスが一体となって、サードパーティのユーザーとハイブリッド環境で勤務する従業員があらゆるデバイスからアクセスできるパブリックホスト名を作成し、保護します。Cloudflareのユーザーレス認証オプション（トークンまたはmTLS証明書）は自動化されたサービスやIoTデバイスの事例にも対応します。

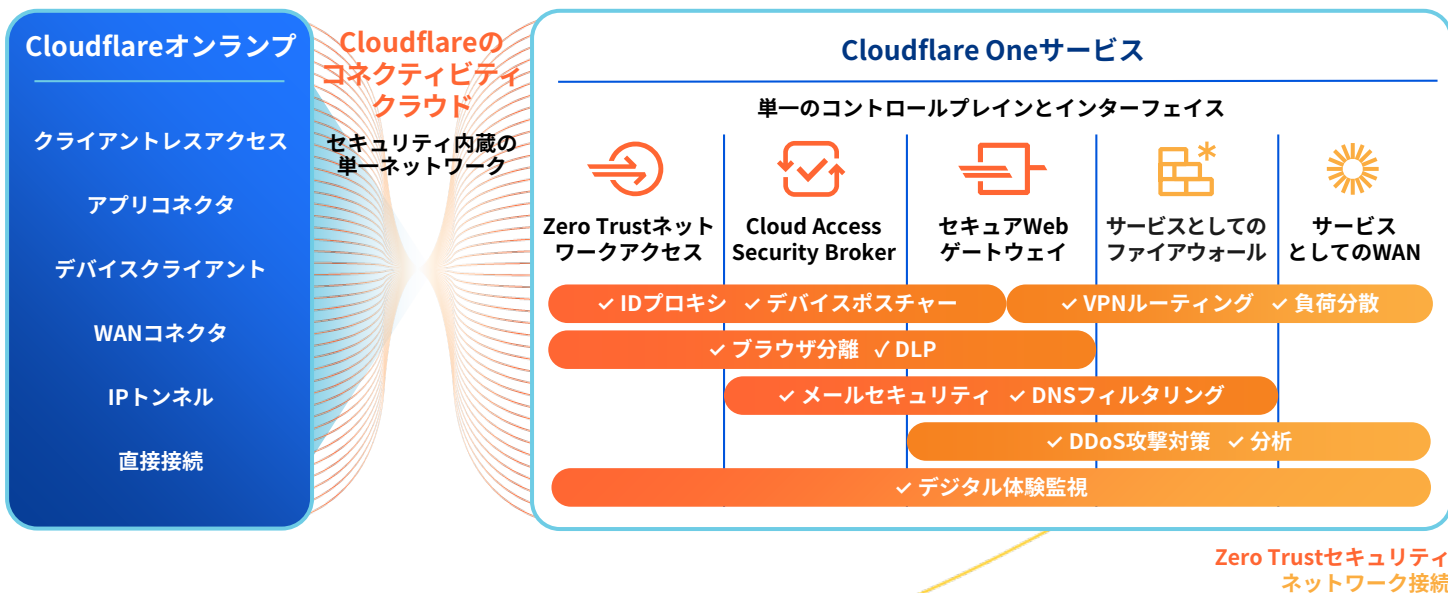
Zero Trustコントロールとリソースでは、セルフホスティングするアプリ（クラウド/オンプレミス）へのリバースプロキシ用にパブリックホスト名かインブラウザのSSH/VNCを、SaaSアプリにはアイデンティティプロキシを、プライベートサブネット内の任意のWebまたはWeb以外（専用TCP/UDP）のリソースにはL4〜L7レイヤーフォワードプロキシ経由によるクライアント/トンネルベースのプライベートルーティングをそれぞれ使用します。Cloudflareのグローバルネットワークとアプリコネクタソフトウェアは、Kubernetes、コンテナ、オンプレミスのレガシーネットワークリソースを含め、パブリッククラウドなどあらゆるコンピューティング環境を総合的にサポートします。その際に、VMインフラストラクチャは必要なく、他のZero Trustベンダーのようなスループット制限も課されません。

サードパーティのアイデンティティ、エンドポイント、ネットワークオンランプ、ログ作成/分析、SIEMツールなどは、デバイスクライアントおよび分析と共に、Cloudflareのダッシュボードに組み込まれています。これにより、管理者は俊敏に対応できるほか、すでに使用しているツールを使って構築できます。

CloudflareのSSEとSASEプラットフォームにアクセス

SSEとSASEでは複数年にわたる戦略的導入工程が発生することもよくありますが、Cloudflareでは企業がZTNAから開始することも珍しくはありません。ZTNAでは、ITチームに実行しやすく、理解しやすいステップが使用され、ビジネスの価値を短期間に示すことができるためです。ITリーダーはハイブリッド環境での勤務体制を保護し、脅威を防御し、統合のためにデータを守る方法を模索しています。また、信頼できるパートナーとしてCloudflareを選択するITリーダーが増えています。

Cloudflareのデプロイの柔軟性と構成可能なアーキテクチャにより、あらゆる企業がデバイス、アプリ、ネットワーク全体のパフォーマンスを保護およびスピードアップすることが可能で、同時にハイブリッド環境の勤務体制を保護し、生産性を向上させることができます。このため、Cloudflareでは、管理者やユーザーの接続元に関係なく、エンドユーザーのエージェントレスオンボーディング、危険なトラフィックを含むクライアントレスWeb分離、セキュリティとネットワークサービス全体を可視化する統合管理ダッシュボードをサポートしています。Cloudflareの広大なグローバルネットワークにより、エンドユーザーに近い場所でセキュリティを適用し、遅延の最小化、従業員に対する円滑なエクスペリエンスの提供を実現しています。Cloudflareのエニーキャストアーキテクチャは、インターネットの混乱を回避する役割を担い、それによってチームのオンライン状態を維持し、ビジネス継続性の確保につなげます。

Cloudflareの統合されたSSEとSASEプラットフォーム、そしてZTNA、CASB、DLP、およびSWGとの間で環境を共有することにより、セキュリティポスチャーを強化するのと同時に、終始一貫した管理ワークフローを通じて実装を簡略化しています。アイデンティティとデバイスポスチャー属性を同一にすることで、ZTNAとCASBの両アクセスポリシーと、SWGポリシーへの通知が可能になり、企業全体でのポリシー管理がシンプルになります。

ZTNA、リモートブラウザ分離、メールセキュリティは、リソースに条件付きのアクセスを提供するために併用できます。その一方でメールやコラボレーションツールを通じて忍び寄る悪意のあるコンテンツ（リンクや添付ファイル）から隔離します。管理対象でないデバイスを使用する請負業者とユーザーには、コーポレートリソースへのユーザーによる操作（アップロード/ダウンロード、コピー/貼り付け、キーボード入力など）を無効にする制限付きアクセスを提供し、データの侵害を回避して、機密データを検出するために他のL7 DLPポリシーを提供することもできます。

お客様の声

「Cloudflare Accessは従来のVPNサービスの代替品として素晴らしい製品です。ユーザーはブラウザを開いてログインするだけ。追加のソフトウェアをダウンロードして設定する必要はありません」

— **Platzi**、クラウドエンジニアリング部長

「社内アセットへのアクセスを制限する場合、AccessはVPNより格段にシンプルで安全です。アクティブにしてユーザーを追加するだけなのに、完ぺきに機能します」

— **Bitpanda**、CTO兼共同設立者

「絶妙なタイミングでCloudflare Accessに出会えたおかげで、面倒なVPNデプロイメントをしなくて済みました。当社にとっては選びやすく、デプロイは驚くほどシンプルでした」

— **ezCater**、セキュリティ責任者

「Cloudflareを実装する前は、アプリケーションを安全にデプロイするための準備に2週間から4週間必要でした。Cloudflare Zero Trustを導入してからこうした時間が約90%も削減されました」

— **Creditas**、ネットワークエンジニアリングチームリード

アナリストの評価：

Cloudflareは2023年の『IDC MarketScape for Zero Trust Network Access（ZTNA）』で「リーダー」に選出

IDCは、Cloudflareの「企業のセキュリティニーズを満たすための積極的な製品戦略」を理由として挙げています。この評価は、どんな規模の企業でもZero Trustの導入を始められ、VPNを使わずにすべてのユーザーをすべてのリソースへ安全に接続できるように支援する当社の姿勢の妥当性が認められたものと、当社は考えています。

Cloudflareは2022年の『KuppingerCole Leadership Compass for ZTNA』で「リーダー」に選出

KuppingerCole Analysts AGは2022年のZTNA市場分析で、有機的に開発され完全統合されたセキュリティプラットフォーム、大規模なグローバルクラウドインフラストラクチャ、圧倒的な市場プレゼンスなど、Cloudflareの強みをいくつか挙げています。

Accessの機能

安全なアクセスのためにZero Trustポリシーを作成/編集する	
きめ細かい、カスタムアクセスポリシー	一元化されたポリシー管理エクスペリエンス。L7アプリはサブドメインとパスレベルでワイルドカードとマルチホスト名サポートで保護、また、CORSリクエストをサポート。ポリシーの変更は数秒でグローバルに拡散。ポリシーテスターを内蔵。
広範なリソース： 保護される対象と仕組み	リソースはセルフホストアプリ（クラウド/オンプレミス）またはインブラウザSSH/VNCへのリバースプロキシにパブリックホスト名を、SaaSアプリにはアイデンティティプロキシを、また、プライベートサブネット内の任意のWeb/Web以外（任意のTCP/UDP）リソースにはL4-7フォワードプロキシ*経由のクライアント/トンネルベースのプライベートルーティングを使用します。
ID	複数の同時IdPを含む、大手企業およびソーシャルアイデンティティプロバイダー（IdP）すべてを経由して認証。汎用SAMLとOIDCコネクタも使用可能。サポート（および強制可能）対象は、IdPで提供される任意のAuthNメソッド、一時AuthN、目的の正当化、re-AuthNインターバルをグローバルまたはアプリセッションベース、およびアプリまたはユーザー別で即座のセッションリボークオプションもあり。
デバイスポスチャー	デバイスクライアントとサードパーティのエンドポイント保護プラットフォーム（EPP）統合を使用してデバイスポスチャーを検証。Zero TrustポリシーにEPPリスクスコアを取り込むには、サービス間統合を使用。
ポリシーのコンテキストシグナル	メールグループ、IPの範囲、ジオロケーション、ログイン方法（MFAタイプ、IdPタイプなど）、有効なmTLSまたはSSH認証、サービストークン、シリアルナンバーリスト、デバイスポスチャー属性、インストール済みのデバイスクライアント、セッション期間、SWGルールの適用などのシグナル、または外部APIコールからのシグナルを設定する。また、Microsoft Entra ID（Azure AD）の条件付きアクセスポリシーを直接参照可能。
他の関連するサポート	• **SCIM：**セルフホスティングやSaaSアプリ（OktaおよびAzure ADなど）にユーザーを自動でプロビジョニング、またはプロビジョニング解除 • **内部DNS：** ローカルドメインフォールバックの設定とプライベートネットワークリクエストの解決 • **スプリットトンネリング：**プライベートネットワークまたはVPNの反対側での実行に IPを含める/除外 • **mTLS認証：**IoTおよび他のmTLSユースケース向けの証明書ベースの認証 • **アプリの分離：**超高速リモートブラウザで1つのチェックボックスによりアプリを分離*
オンランプとオフランプ	
アプリコネクタ	シンプルなオーケストレーションを実現する軽量なアプリコネクタ（Cloudflare Tunnel）がVMインフラストラクチャやスループットの必要なく、Cloudflareへのリソースの接続を円滑化。モニタリング、仮想ネットワーク（IPオーバーラップ用）、冗長性、フェイルオーバー機能を含む。
デバイスクライアント： 使用するタイミング	• **クライアントレス：**Zero Trustのポリシーを管理対象デバイスのサードパーティユーザーに拡張。さらにクライアントレスRBIおよびL7 DLPポリシー*と併用。クライアントレスアクセスはWebアプリとインブラウザSSH/VNCに対応。 • **クライアントベース：**デバイスクライアント（Cloudflare WARP）がプライベートネットワークへ安全なアクセスを拡張し、サービス間のデバイスポスチャーの統合を実現。また、オンプレミスのユーザーに場合に応じたポリシーを適用するために位置認識機能を装備。プライベートネットワークを作成するために、2つまたは3つのWARPを実行する任意のデバイスに接続可能。ユーザーは自己登録またはMDM経由でデプロイ可能。
拡張性と可視性	
ページのカスタマイズ	自社のブランディング、またはエンドユーザーエクスペリエンスを効率化するために個々のアクセス手順を挿入するブロックおよびアプリランチャー画面にカスタムHTMLをアップロード。
ログ	包括的ログですべてのリクエスト、ユーザー、デバイスのログを記録。logpushまたはAPIを使用して既存のSIEM、オーケストレーション、分析ツールと統合可能。不明なアセットには社内インフラストラクチャ用シャドーITがユニークなトラフィックを受動的にカタログ化することで、すべてのオリジンを表面化。
自動化	直感的なAPIとTerraformプロバイダーが利用可能で、Zero Trustの実装に伴うあらゆる側面をプログラム的に管理。また、自動化されたサービスをサポートするためにユーザーレスサービストークンを提供。

**Zero Trustプラットフォームの他の部分で機能を使用*

Cloudflareを選ぶ理由

簡単なセットアップと管理

アプリコネクタソフトウェアとトンネルオーケストレーションを使用して、プライベートリソースへのオンラントラフィックの設定と運用を根本から簡素化します。

シームレスな常時接続体験

Cloudflareのグローバルなエニーキャストテクノロジーにより、エンドユーザーのピークパフォーマンスとネットワーク障害への耐性を実現し、信頼性を確保します。

アーリーアダプターによる迅速なイノベーション

より速く、より安全なアプリへのアクセスを目指して常に同業他社を凌駕する革新を行うプロバイダーと共に、インターネットそのものの進化と足並みを揃えます。

お客様の企業にとっての簡単かつ安全なアクセスについてご不明な点やご要望をお聞かせください

ワークショップを依頼する

相談の前に資料をご覧になりたい方は、

CloudflareのSSEとSASEプラットフォームについてさらに詳しくご覧ください

1. 2023年調査：techvalidate.com/product-research/cloudflare/charts